



1FW

## PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Kyung-Hee LEE et al.

Docket: 678-1395

Serial No.: 10/800,181

Dated: July 26, 2004

Filed: March 12, 2004

For: APPARATUS AND METHOD FOR PERFORMING  
MONTGOMERY TYPE MODULAR MULTIPLICATIONCommissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to Applicants' duty of disclosure, the information listed in the attached form PTO-1449 is brought to the attention of the Examiner. A copy of each reference is attached hereto.

The citation of the listed items is not a representation that they constitute a complete or exhaustive listing of the relevant art or that the references are prior art. The items listed are submitted in good faith, but are not intended to substitute for the Examiner's search. It is hoped, however, that in addition to apprising the Examiner of these particular items, they will assist in identifying fields of search and in making as full and complete a search as possible.

---

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postpaid in an envelope, addressed to the: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 26, 2004.

Dated: July 26, 2004  
Paul J. Farrell

The filing of this Information Disclosure Statement is not an admission that the information cited herein is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

To the best of Applicants' knowledge, this Information Disclosure Statement is being filed before the date of mailing of a first Office Action in connection with this case.

The claims of the application as now presented are believed to patentably distinguish over the prior art and to be in condition for allowance. Early and favorable consideration of the case is respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Paul J. Farrell", written in a cursive style.

Paul J. Farrell

Reg. No. 33,494

Attorney for Applicants

**DILWORTH & BARRESE, LLP**  
333 Earle Ovington Blvd.  
Uniondale, NY 11553  
(516) 228-8484



Form PTO-1449

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICEATTY. DOCKET NO.  
678-1395SERIAL NO.  
10/800,181INFORMATION DISCLOSURE  
STATEMENT BY APPLICANTAPPLICANTS  
Kyung-Hee LEE et al.FILING DATE  
March 12, 2004GROUP ART UNIT  
Not Yet Assigned

(Use several sheets if necessary)

## U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	6,185,596	2/6/2001	Hadad et al.			

## FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO

## OTHER PRIOR ART (Including Author, Title, Date, Pertinent Pages, Etc.)

		1.	Rivest et al., "A Method of Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, February 1978, Vol. 21, No. 2, pp. 120-126.
		2.	Montgomery, "Modular Multiplication Without Trial Division", Mathematics of Computation, Vol. 44, No. 170, April 1985, pp. 519-521.
		3.	Dusse et al., "A Cryptographic Library for the Motorola DSP56000", Advances in Cryptology - EUROCRYPT '90, pp. 230-244.
		4.	Bosselaers et al., "Comparison of Three Modular Reduction Functions", Advances in Cryptology - CRYPTO '93, pp. 175-186.

EXAMINER

DATE CONSIDERED

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Form PTO-1449 [6-4])